UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/925,503	08/10/2001	Victor I. Sheymov	741946-30	7363

22204 7590 05/04/2005

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/925,503	SHEYMOV, V. ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-30 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-30 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 10 August 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 20020716, 20040728.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-30 are pending.

Claim Objections

1. Claims 9, 19, and 22-30 are objected to under 37 CFR 1.75(a) because of the following informalities:

- Claim 9 should read as follows: "The system of claim 8, wherein the one or more entities attempting the unauthorized access are unaware that they are communicating with the at least one destination."
- Claim 19 should read as follows: "The method of claim 18, wherein the one or more entities attempting the unauthorized access are unaware that they are communicating with the at least one destination."
- Claims 22, 24-26, 28, and 30 should be dependent upon claim 21.
- Claim 23 should be dependent upon claim 22.
- Claim 27 should be dependent upon claim 26.
- Claim 29 should read as follows: "The media of claim 28, wherein the one or more entities attempting the unauthorized access are unaware that they are communicating with the at least one destination."

Appropriate correction is required.

Claim Rejections - 35 USC § 101

2. Claims 21-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In order to be statutory subject matter, the claims must recite a computer readable medium that contains executable code.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 11-13, and 21-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Bernhard (U.S. Patent 6,275,942).

Regarding Claim 1,

Bernhard et al. disclose a network protection system comprising:

A communications management system [firewall] (Column 4, line 50 to Column 5, line 7); and

An analysis system [ARM] wherein the analysis system receives information associated with an unauthorized access attempt and at least one of forwards a portion of the received information to at least one destination and forwards instructions to an intrusion detection system (Column 5, lines 47-63).

Regarding Claim 11,

Claim 11 is a method claim that corresponds to system claim 1 and is rejected for the same reasons.

Regarding Claim 21,

Claim 21 is a media claim that corresponds to system claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Bernhard et al. disclose that the information associated with an unauthorized access attempt is received from an intrusion detection system (Column 5, lines 47-63).

Regarding Claim 12,

Claim 12 is a method claim that corresponds to system claim 2 and is rejected for the same reasons.

Regarding Claim 22,

Claim 22 is a media claim that corresponds to system claim 2 and is rejected for the same reasons.

Regarding Claim 3,

Bernhard et al. disclose that the intrusion detection system at least detects one or more unauthorized access attempts (Column 5, lines 47-63).

Regarding Claim 13,

Claim 13 is a method claim that corresponds to system claim 3 and is rejected for the same reasons.

Regarding Claim 23,

Claim 23 is a media claim that corresponds to system claim 3 and is rejected for the same reasons.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 4, 14, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bernhard in view of Rowland (U.S. Patent 6,405,318).

Regarding Claim 4,

Bernhard et al. do not disclose that the analysis system verifies the legitimacy of one or more access attempts.

Rowland, however, discloses that the analysis system verifies the legitimacy of one or more access attempts (Column 7, line 55 to Column 8, line 7). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the user profiling method of Rowland into the intrusion detection system of Bernhard et al. in order to

reduce the amount of false positives generated by the intrusion detection system, thus incurring less processing and analysis time being wasted on an event which isn't actually an intrusion attempt (Column 1, lines 21-49; and Column 2, line 40 to Column 3, line 3).

Regarding Claim 14,

Claim 14 is a method claim that corresponds to system claim 4 and is rejected for the same reasons.

Regarding Claim 24,

Claim 24 is a media claim that corresponds to system claim 4 and is rejected for the same reasons.

5. Claims 5, 6, 8-10, 15, 16, 18-20, 25, 26, and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bernhard in view of Joyce (U.S. Patent 6,519,703).

Regarding Claim 5,

Bernhard et al. do not disclose that the analysis system communicates information regarding an unauthorized access attempt to a monitoring center.

Joyce, however, discloses that the analysis system communicates information regarding an unauthorized access attempt to a monitoring center (Column 2, line 55-65; and Column 4, line 61 to Column 5, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the heuristic analysis system of Joyce

into the intrusion detection system of Bernhard et al. in order to monitor and reveal previously unknown attacks, thus allowing the intrusion detection system to detect and prevent this new form of attack in the future and to determine incriminating evidence against the attacker, such as their source.

Regarding Claim 15,

Claim 15 is a method claim that corresponds to system claim 5 and is rejected for the same reasons.

Regarding Claim 25,

Claim 25 is a media claim that corresponds to system claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Bernhard et al. do not disclose that the analysis system communicates with the at least one destination via a communications link.

Joyce, however, discloses that the analysis system communicates with the at least one destination via a communications link (Column 2, lines 55-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the heuristic analysis system of Joyce into the intrusion detection system of Bernhard et al. in order to monitor and reveal previously unknown attacks, thus allowing the intrusion detection system to detect and prevent this new form of attack in

the future and to determine incriminating evidence against the attacker, such as their source.

Regarding Claim 16,

Claim 16 is a method claim that corresponds to system claim 6 and is rejected for the same reasons.

Regarding Claim 26,

Claim 26 is a media claim that corresponds to system claim 6 and is rejected for the same reasons.

Regarding Claim 8,

Bernhard et al. do not disclose that the analysis system enables communication between the at least one destination and one or more entities attempting the unauthorized access attempt.

Joyce, however, discloses that the analysis system enables communication between the at least one destination and one or more entities attempting the unauthorized access attempt (Column 2, line 55-65; and Column 4, line 61 to Column 5, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the heuristic analysis system of Joyce into the intrusion detection system of Bernhard et al. in order to monitor and reveal previously unknown attacks, thus allowing the intrusion detection system to detect and prevent this new form of attack in the future and to

determine incriminating evidence against the attacker, such as their source.

Regarding Claim 18,

Claim 18 is a method claim that corresponds to system claim 8 and is rejected for the same reasons.

Regarding Claim 28,

Claim 28 is a media claim that corresponds to system claim 8 and is rejected for the same reasons.

Regarding Claim 9,

Joyce discloses that the one or more entities attempting the unauthorized access are unaware that they are communicating with the at least one destination (Column 2, lines 55-65).

Regarding Claim 19,

Claim 19 is a method claim that corresponds to system claim 9 and is rejected for the same reasons.

Regarding Claim 29,

Claim 29 is a media claim that corresponds to system claim 9 and is rejected for the same reasons.

Regarding Claim 10,

Bernhard et al. do not disclose that the communications from the at least one destination are modified to appear as if they have a predetermined origin.

Joyce, however, discloses that the communications from the at least one destination are modified to appear as if they have a predetermined origin (Column 2, lines 55-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the heuristic analysis system of Joyce into the intrusion detection system of Bernhard et al. in order to monitor and reveal previously unknown attacks, thus allowing the intrusion detection system to detect and prevent this new form of attack in the future and to determine incriminating evidence against the attacker, such as their source.

Regarding Claim 20,

Claim 20 is a method claim that corresponds to system claim 10 and is rejected for the same reasons.

Regarding Claim 30,

Claim 30 is a media claim that corresponds to system claim 10 and is rejected for the same reasons.

6. Claims 7, 17, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bernhard in view of Joyce, further in view of Cheng et al. (U.S. Patent 6,738,909).

Regarding Claim 7,

Bernhard et al. as modified by Joyce does not disclose that the communications link is a secure tunnel.

Cheng et al., however, disclose a communications link being a secure tunnel (Column 6, lines 11-22). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the secure tunnel of Cheng et al. into the intrusion detection system of Bernhard et al. as modified by Joyce in order to protect the data for integrity, authenticity, and confidentiality.

Regarding Claim 17,

Claim 17 is a method claim that corresponds to system claim 7 and is rejected for the same reasons.

Regarding Claim 27,

Claim 27 is a media claim that corresponds to system claim 7 and is rejected for the same reasons.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER